# Семинар №4. Кольца, поля, полукольца

Теоретический материал: гл. 2, 2.3, 2.6; гл.3, 3.1-3.3. Статья: *Белоусов А.И.* О некоторых свойствах полуколец (выложена на персональной странице автора).

**Задача №1** (2.9, стр. 172). Является ли полем множество чисел вида , где  (рациональные числа) с обычными операциями сложения и умножения.

**Решение**

Свойства числовых операций проверять не нужно: они известны. Здесь нужно убедиться в том, что определенное в условии задачи множество  замкнуто относительно операций сложения и умножения, то есть сумма и произведение двух чисел из  принадлежит .

Это легко проверить:



Кроме этого, нейтральные элементы 0 и 1 представляются как числа из этого же множества :

.

Множество можно уподобить множеству комплексных чисел, у которых есть действительная и мнимая части. Здесь же мы можем говорить о рациональной и иррациональной части.

Итак, мы имеем числовую алгебру , которая, очевидно, является кольцом и подалгеброй поля действительных чисел.

Чтобы ответить на вопрос, является ли это кольцо полем, нужно проверить обратимость по умножению произвольного ненулевого числа из множества .

Имеем:

.

Знаменатель этой дроби не может оказаться равным нулю, так как тогда мы получили бы, что , но отношение рациональных чисел не может быть иррациональным числом.

Итак, любой ненулевой элемент множества  обратим по умножению, и

,

так как обе дроби в написанной выше формуле являются рациональными числами (что совершенно очевидно).

Итак, алгебра есть поле. Оно является расширением поля рациональных чисел (то есть содержит последнее в качестве подполя).

**Задача №2** (2.12, стр. 173). Кольцо  называется булевым, если его умножение идемпотентно, то есть для любого  Доказать, что:

1) , то есть любой элемент противоположен сам себе: ;

2) любое булево кольцо коммутативно;

3) в любом булевом кольце, имеющем более двух элементов, есть делители нуля.

**Решение**

1) Рассмотрим выражение 

Но одновременно  То есть , откуда и получаем .

2) Преобразуем выражение 

Но так как , то есть , откуда , и, в силу свойства (1), .

3) Рассмотрим произведение , полагая, что  (что возможно, так как по условию в носителе кольца не менее трех элементов, то есть кроме 0 и 1 есть еще какие-то элементы). Тогда в записанном выше произведении оба сомножителя отличны от нуля, а их произведение равно нулю: , что и доказывает утверждение п. 3.

Задача решена.

**Замечание**. Булевым кольцом является кольцо подмножеств произвольного множества -

.

Делителями нуля в нем будут два любых непересекающихся множества (которые всегда найдутся, если в исходном множестве не менее двух элементов).

Булевым кольцом будет также поле вычетов по модулю 2 (поле ), причем это единственное поле вычетов, являющееся одновременно булевым кольцом.

**Системы линейных уравнений в поле вычетов**

**Задача №3**. Решить систему линейных уравнений в поле :



**Решение**

Решаем стандартно методом Гаусса, но с учетом того, что все вычисления проводятся по модулю 23, то есть везде в качестве результата пишем остаток от деления на 23 (или противоположный к нему в данном поле).

Запишем основную и расширенную матрицу, упростив 2-ю строку использованием противоположных элементов:

 .

Первое элементарное преобразование состоит в том, что ко 2-й строке прибавляется 1-я, умноженная на 2, а из 3-й строки вычитается 1-я, умноженная на 5.

В результате получим матрицу:

.

Теперь к 3-й строке, умноженной на 3, прибавляем 2-ю:

.

Привели основную матрицу к верхнетреугольной форме, получив тем самым уравнение для z:

, или, что то же самое:

.

Сокращая на 2, получим:

.

Тогда



(Не пишем никаких дробей! Никаких 2/7!).

Мультипликативная операция нашего поля обозначена просто точкой, которую зачастую опускают. Ниже будет приведен один из алгоритмов вычисления мультипликативных обратных в полях вычетов, но в данном случае его легко угадать: 7х10=70=1 (mod 23).

**Замечание**. Еще проще, если догадаться, что 2 = -21. Тогда сразу сокращаем на 7 и получаем -3.

Уравнение для y:



Находим x:



Сделаем проверку:

2-5(-5)-3=1,

(-2)2+4(-5)+3=-1+3=2,

5(2)-6(-3)=10+18=5.

Верно.

Ответ: 

Вычисление мультипликативных обратных в полях вычетов

Согласно малой теореме Ферма (см. п. 2.7, стр. 155-157) для любого ненулевого элемента поля  выполняется . Умножая это равенство на обратный к , получим  . Это и есть формула для вычисления обратного по умножению. Показатель степени можно взять по модулю порядка данного элемента, если он окажется меньше порядка мультипликативной группы поля, то есть числа p-1.

Например, при решении системы в предыдущей задаче мы могли бы вычислить обратный к 7 следующим образом (разложив показатель степени на сумму степеней двойки):



Все вычисления выполняются по модулю 23! В данном конкретном случае проще было обратный угадать, ответив на нехитрый вопрос: на какое число надо умножить 7, чтобы в результате получилось число, при делении на 23 дающее остаток 1? Ясно, что этот неизвестный множитель есть 10.

Можно было предварительно вычислить порядок 7 в данном поле. Здесь рассуждаем так. Порядок любого элемента конечной группы, в силу теоремы Лагранжа (п. 2.7), должен быть делителем порядка всей мультипликативной группы поля вычетов. В данном случае это 22. Нетривиальных делителей у числа 22 два: 2 и 11. Но . Вычисляем . Поскольку число 11 простое, то 11-я степень 7 – наименьшая положительная степень 7, дающая -1. Значит, порядок 7 равен 22, то есть порядку всей группы . В качестве побочного результата получаем, что группа  циклическая, и 7 – один из ее образующих элементов.

**Замечания**. 1) Замечание по поводу простого показателя степени (11) выше имеет такой смысл. Порядок элемента  конечной группы можно найти, вычислив наименьший положительный показатель степени такой, что . Тогда понятно, что порядок элемента будет равен . Но надо быть уверенным в том, что - наименьший показатель степени с таким свойством. Если это простое число, то так и есть. В случае составного  это может быть неверно. Например, пусть в группе  для некоторого  получилось . Но , и может оказаться, что  или .

2) **Важно не перепутать**: *при вычислении целых степеней элементов мультипликативных групп вычетов (то есть мультипликативных групп полей вычетов , где  - простое число) показатель степени следует брать по модулю порядка группы, то есть числа , но все вычисления проводить по модулю *.

Можно проверить, что порядок 8 в группе  равен 11 (проверить!). Тогда, например,

.

Вычисления проводим по модулю 23! И используем переход к противоположному элементу.

Например,  в аддитивной группе поля. Также используем в вычислениях то свойство, что в любом кольце произвольная четная степень взаимно противоположных элементов дает один и тот же результат – как в обычной арифметике. В частности, для любого  . Рекомендуется это доказать самостоятельно.

**Системы линейных уравнений в полукольцах с тривиальной итерацией**

Полукольцо  называется полукольцом с тривиальной итерацией, если итерация любого элемента в нем равна единице полукольца.

В таких полукольцах легко решать системы линейных уравнений, так как для линейного уравнения вида



наименьшее решение, даваемое формулой , совпадает со свободным членом:

.

**Задача №4**

В полукольце  решить систему



Для удобства записи мы переобозначили операции: + означает max, а точка (как правило, опускаемая) – min. То есть .

**Решение**

Действуя по схеме последовательного исключения неизвестных (стр. 199-201), получим, исключая :

,

Так как итерация любого элемента в этом полукольце с тривиальной итерацией есть единица полукольца – нейтральный элемент по умножению.

Подставляя полученное выражение во 2-е и 3-е уравнения, получим:



После приведения подобных членов в правых частях будем иметь:



Исключаем второе неизвестное:

.

Подставляя это в уравнение для 3-го неизвестного, получим:



Тогда 

.

Ответ: .

Заметим, что рассматриваемое полукольцо является симметричным (п. 3.4), и алгебра

 также полукольцо (с тривиальной итерацией), называемое двойственным к исходному.

Рекомендуется самостоятельно решить ту же систему в этом двойственном полукольце, понимая теперь уже + как min, а точку как max.

**Задача №5**

Решить в полукольце  делителей числа 200 по операциям НОК и НОД систему



**Решение**

Поскольку это полукольцо также является полукольцом с тривиальной итерацией, то действуем так же, как и предыдущей задаче. Обозначения операций изменены, как и в предыдущей задаче: + означает НОК (наименьшее общее кратное), точка (обычно опускаемая) – НОД (наибольший общий делитель).

Из первого уравнения выражаем первое неизвестное через остальные:

.

Подставим это выражение во 2-е и 3-е уравнения:



Приводя подобные члены в правых частях, получим:



Далее:



Ответ: .

Предлагается самостоятельно решить ту же систему в двойственном полукольце

,

то есть + есть НОД, точка – НОК.

**Замечание**. Такие системы в полукольцах с тривиальной итерацией можно решать несколько быстрее, отклоняясь от строгого следования схеме последовательного исключения неизвестных.

Можно сразу зачеркнуть все «рекурсивные» слагаемые в правых частях, то есть те, которые содержат неизвестное, стоящее слева. И можно не заботиться о них при приведении подобных членов.

Тогда решение задачи №4 будет выглядеть так:



(переписали исходную систему без рекурсивных слагаемых).

Делаем подстановку выражения для первого неизвестного во второе и третье уравнения:



Но при приведении подобных не выписываем слагаемое с  в первом уравнении и слагаемое с во втором:



Уравнение для :

,

откуда сразу получаем



Остальные неизвестные определяются, как выше.

Но использовать такую упрощенную схему рекомендуется всё же при достаточном опыте записи подробных решений, с использованием полной «схемы Гаусса».

**Задачи для самостоятельного решения**

1) Решить системы линейных уравнений:

 в ;

 в .

2) Найти элемент, обратный к по умножению, в поле . Является ли циклическая подгруппа, порожденная элементом , всей группой ?

а) ;

б) ;

в) .

3) Задача 3.3 (к главе 3, стр. 223)

4) Более трудные задачи: 2.14, 2.15, 2.16 и 2.19.

**Указания**

**2.15(б)**

Пусть ненулевой элемент  кольца без делителей нуля обратим слева, то есть существует такой элемент  (левый обратный) такой, что . Тогда ,

но так как , то (нет делителей нуля!), и , то есть левый обратный является и правым обратным для .

Аналогично доказывается, что из существования правого обратного следует, что он совпадет в таком кольце с левым обратным.

Чтобы доказать аналогичное утверждение для конечного кольца, используйте отображение сдвига, как это сделано в доказательстве теоремы 2.9 (п. 2.4, стр. 141).

Именно, предполагая, что ненулевой элемент конечного кольца обратим слева, то есть, что существует такой элемент  (левый обратный) такой, что , определим отображение (левого сдвига на ) множества ненулевых элементов кольца в себя так, что  Докажем, что это инъекция.

Пусть . Тогда . Умножая это равенство на  слева, получим  Но инъекция конечного множества в себя есть биекция, откуда каждый ненулевой элемент кольца имеет единственный прообраз при отображении левого сдвига. В том числе, для единицы получим, что существует такой ненулевой , что , и этот  и есть правый обратный к . Остается показать, что он совпадает с левым обратным (самостоятельно!).

Подобным же рассуждением доказывается, что правый обратный, существующий по предположению, совпадает с левым обратным.

**2.16(а)**

Пусть оба произведения  и обратимы. Обозначим соответствующие обратные как  и  соответственно.

Тогда , что означает, что элемент  есть правый обратный к . Левый обратный для  и оба обратных для  найдите самостоятельно.

### Дополнения

## Доказательство ассоциативности операции min (для чисел)

Надо доказать, что для любых вещественных чисел *a*, *b* и *с*

.

**Случай 1**: 

Тогда

,

.

**Случай 2**: 

,



## Доказательство дистрибутивности min относительно max

Надо доказать, что для любых вещественных чисел *a*, *b* и *с*

.

Случай 1. 

* 1. 

,

.

1.2 

,

.

1.3 

,



Случай 2. 

2.1 

,

.

2.2 

,

.

2.3 

,

.

Доказано.

Доказательство дистрибутивности числового сложения относительно операции min приведено в Учебнике, стр. 168 (по 7 изд, п. 3.1).

## Доказательство теоремы Эйлера

***Теорема Эйлера***: *для любого натурального k и целого a, взаимно простого с k, число a*ϕ*(k) =* 1 *(mod k), где* ϕ*(k) – количество всех натуральных чисел, взаимно простых с k и меньших k*.

(Заметим, что для простого *k* значение ϕ*(k)* = *k* -1, и мы получаем частный случай теоремы Эйлера, известный как ***малая теорема Ферма***).

♦Разложим число *a* по модулю *k*, представив его в виде *a=mk*+*r*, где 0 < *r* < *k*. Воспользовавшись формулой бинома Ньютона, получим

(*mk+r*) ϕ*(k)*=(*mk*) ϕ*(k)*+…+ ϕ(*k*) (*mk*)*r*ϕ*(k)-*1+ *r*ϕ*(k)*= *r*ϕ*(k)* (mod k).

Более того, число *r* взаимно просто с *k*. Действительно, если бы это было не так, то указанные числа имели бы общий делитель *s>*1, но тогда и сумма *mk*+*r* делилась бы на *s*, и числа *a* и *k* не были бы взаимно простыми. Следовательно, *r* есть элемент группы всех обратимых элементов кольца **Z**k. Рассмотрим тогда в этой группе циклическую подгруппу, порожденную элементом *r*. Ее порядок *l*, равный порядку ее образующего элемента, т.е. *r*, по теореме Лагранжа есть делитель порядка всей группы обратимых элементов кольца **Z**k, который равен ϕ(*k*). Т.е. для некоторого целого *q* выполняется ϕ(*k*)=*ql*. Следовательно, мы имеем: *r*ϕ*(k)*=*rql=(rl)q=*1 (mod k), что и требовалось доказать. ♦

## Образующие элементы конечной циклической группы

*Если  - образующий элемент конечной циклической группы порядка , то его степень будет образующим тогда и только тогда, когда число  взаимно просто с *

(См. лекцию №11.)

◄Пусть нашлось число , что для некоторого , выполняется . Ясно, что , но, ввиду взаимной простоты чисел  и , . Следовательно, . Пусть  кратно , но тогда, поскольку не делится на , а , то оба этих числа,  и , должны иметь отличные от 1 и от  делители , что, очевидно, невозможно по условию. Итак, не делится на , и, раскладывая по модулю , получим: . Тогда , что невозможно, так как .

Утверждение доказано►.

**Замечание**. Можно доказать, что *только* степени элемента , взаимно простые с , будут порождать группу.

Действительно, пусть . Тогда для некоторых и имеем и , то есть существует меньшая степень элемента , а именно , равная единице, то есть порядок меньше n и он не порождает всю группу.